

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
11. August 2005 (11.08.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/074189 A1

(51) Internationale Patentklassifikation⁷: **H04L 9/32**,
29/06

(DE). VOLKMANN, Gerald [DE/DE]; Fontanestr. 29a,
15344 Strausberg (DE).

(21) Internationales Aktenzeichen: PCT/EP2005/050360

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGE-
SELLSCHAFT**; Postfach 22 16 34, 80506 München
(DE).

(22) Internationales Anmeldedatum:
28. Januar 2005 (28.01.2005)

(25) Einreichungssprache: Deutsch

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES,
FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,
ZW.

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 004 606.9 29. Januar 2004 (29.01.2004) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): **SIEMENS AKTIENGESELLSCHAFT** [DE/DE];
Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

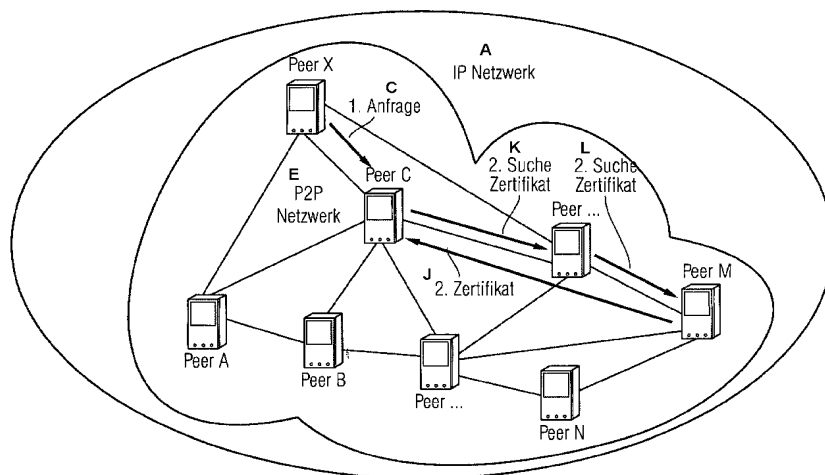
(75) Erfinder/Anmelder (nur für US): **BUSSER, Jens, Uwe**
[DE/DE]; Gustav-Heinemann-Ring 98, 81739 München

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,

[Fortsetzung auf der nächsten Seite]

(54) Title: CIRCUIT ARRANGEMENT AND METHOD FOR SECURING COMMUNICATION WITHIN COMMUNICATION
NETWORKS

(54) Bezeichnung: SCHALTUNGSANORDNUNG UND VERFAHREN ZUR KOMMUNIKATIONSSICHERHEIT
INNERHALB VON KOMMUNIKATIONSNETZEN



A... IP NETWORK
C... 1. QUESTION
E... P2P NETWORK
J... CERTIFICATE
K... 2.SEARCH CERTIFICATE
L... 2.SEARCH CERTIFICATE

(57) Abstract: The invention relates to a circuit arrangement and associated method for the authentication of a network subscriber. A digital certificate is stored as a resource in the P2P network. The advantage thereof is that data can be also be provided for the other network subscribers, when the network subscriber(s) are offline or can not be reached for other reasons. It is also possible to encode data which is specific for other network units and file said data in a protective manner for the P2P network.

[Fortsetzung auf der nächsten Seite]

WO 2005/074189 A1



GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Veröffentlicht:

— mit internationalem Recherchenbericht

(57) Zusammenfassung: Bei dieser Schaltungsanordnung und dem dazugehörigen Verfahren zur Authentisierung eines Netzteilnehmers wird ein digitales Zertifikat als Ressource im P2P-Netzwerk abgespeichert. Dies bringt den Vorteil mit sich, dass Daten auch dann den weiteren Netzteilnehmern zur Verfügung gestellt werden können, wenn die oder der Netzteilnehmer im Betriebsmodus Offline oder aus anderen Gründen nicht erreichbar ist. Des weiteren ist es auch möglich, für Netzeinheiten bestimmte Daten verschlüsselt und somit geschützt im P2P-Netzwerk abzuliegen.

Beschreibung

Schaltungsanordnung und Verfahren zur Kommunikationssicherheit innerhalb von Kommunikationsnetzen

5

In modernen Kommunikationsnetzen gewinnt die Kommunikationssicherheit zunehmend an Bedeutung. Dabei sind wichtige Aspekte der Kommunikationssicherheit die Authentizität der Teilnehmer und die Vertraulichkeit von Nachrichten. Zur Teilnahme an einer Kommunikation innerhalb von Netzwerken kann außerdem eine Autorisierung erforderlich sein. Diese Kommunikationssicherheit wird üblicherweise mit voradministrierten, gemeinsamen Geheimnissen wie beispielsweise shared secrets verwirklicht. Des weiteren kann auch mit digitalen Signaturen/Zertifikaten die Kommunikationssicherheit gewährleistet werden. Dabei erhält jeder zur sicheren Kommunikation autorisierte Netzteilnehmer ein eigenes digitales Zertifikat von einer vertrauenswürdigen zentralen Instanz. Diese Zertifikate binden einen öffentlichen Schlüssel an die Identität seines Eigentümers. Diese Zertifikate können überprüft werden mit dem öffentlichen Schlüssel der zentralen Instanz, der im sogenannten Root-Zertifikat der zentralen Instanz enthalten ist, welches unverfälscht an alle Netzwerkteilnehmer verteilt werden muss. Ein Netzteilnehmer kann nun mit seinem geheimen privaten Schlüssel eine signierte Nachricht erzeugen, deren Authentizität von jedem Empfänger mittels des öffentlichen Schlüssel aus dem Zertifikat des Netzteilnehmers geprüft werden kann. Das Zertifikat eines Netzteilnehmers erhält der Empfänger entweder von Netzteilnehmer selbst oder von einem zentralen Server. Zur vertraulichen Übermittlung von Nachrichten werden diese mit dem öffentlichen Schlüssel aus dem Zertifikat des Empfängers verschlüsselt, so dass nur dieser die Nachricht wieder entschlüsseln kann.

35 In einem Peer-to-Peer Netzwerk, nachfolgend mit P2P Netzwerk abgekürzt, finden Sicherheitsfunktionen wie Authentisierung, Autorisierung und Ver-/Entschlüsselung ebenso Anwendung. Wer-

den danach Informationen aus dem Zertifikat eines Netzteilnehmers benötigt, so kann das Zertifikat von dieser Netzeinheit selbst oder falls vorhanden von einer externen Speichereinheit angefordert werden.

5

Die bisher beschriebene Authentisierung von Daten oder Nachrichten einer Netzeinheit in einem P2P Netzwerk bringt jedoch den Nachteil mit sich, das ein Zertifikatsserver für die Teilnehmer des P2P Netzwerks zur Verfügung stehen muss

10

und/oder die Netzteilnehmer ständig im Online-Betrieb sich befinden müssen. Darüber hinaus können auch keine vertraulichen Nachrichten für Netzteilnehmer allgemein noch für bestimmte Netzteilnehmer hinterlegt werden, wenn oben genannte Netz- und Netzteilnehmerbedingungen vorliegen.

15

Der Erfindung liegt die Aufgabe zugrunde, eine Schaltungsanordnung und ein dazugehöriges Verfahren zur Absicherung der Kommunikation von Netzteilnehmern anzugeben.

20

Die Aufgabe wird durch die Merkmale der Ansprüche 1 und 4 gelöst.

Die Erfindung bringt den Vorteil mit sich, dass eine Authentizitätsprüfung auch bei einem Offline-Betrieb des Netzteilnehmers durchgeführt werden kann.

25

Die Erfindung bringt den Vorteil mit sich, dass eine Autorisierungsprüfung über das Zertifikat des Netzteilnehmers auch bei einem Offline-Betrieb des Netzteilnehmers durchgeführt werden kann.

30

Die Erfindung bringt den Vorteil mit sich, dass eine vertrauliche Informationshinterlegung auch in einem Offline-Betrieb des Netzteilnehmers im P2P Netzwerk durchgeführt werden kann.

35

Die Erfindung bringt den Vorteil mit sich, dass Server zur Bereitstellung von erstellten und abgespeicherten Zertifika-

ten im laufenden Betrieb nicht erforderlich sind.

Weitere Besonderheiten der Erfindung werden aus den nachfolgenden näheren Erläuterungen zu den Figuren eines Ausführungsbeispiels ersichtlich.

Es zeigen:

Figur 1 ein P2P-Netzwerk innerhalb eines IP-Netzwerkes,
Figur 2 eine Zuteilung eines Zertifikates für einen neuen
10 Netzteilnehmer und deren Verteilung im P2P-Netzwerk,
Figur 3 eine schematische Darstellung der Authentisierung
der Nachricht eines Netzteilnehmers,
Figur 4 einen Aufbau von Schaltungsmodulen innerhalb eines
Peers,
15 Figur 5 ein Ablaufdiagramm einer Zertifikatsverteilung,
Figur 6 ein Ablaufdiagramm einer Authentizitätsprüfung und
Figur 7 ein Ablaufdiagramm einer verschlüsselten Hinterlegung.

20 Anhand einer Schaltungsanordnung und dem dazugehörigen Verfahren zur Authentisierung eines Netzteilnehmers wird ein digitales Zertifikat als Ressource im P2P-Netzwerk abgespeichert. Dies bringt den Vorteil mit sich, dass Daten auch dann
25 den weiteren Netzteilnehmern zur Verfügung gestellt werden können, wenn die oder der Netzteilnehmer im Betriebsmodus Offline oder aus anderen Gründen nicht erreichbar ist. Des weiteren ist es auch möglich, für Netzeinheiten bestimmte Daten verschlüsselt und somit geschützt im P2P-Netzwerk abzulegen.
30

Figur 1 zeigt ein P2P-Netzwerk innerhalb eines mit IP bezeichneten Netzwerkes.

Der Datentransfer bis zur Transportschicht findet über gebräuchliche Protokolle, beispielsweise das Internetprotokoll,
35 statt. Zwischen dieser Transportschicht und der Anwendungsschicht befindet sich als zusätzliche Schicht die Schicht des

P2P Protokolls, welche die Zuordnung von Identifikation ID zu anderen Teilnehmern und Datensätzen vornimmt, das Abspeichern, Extrahieren sowie die Replikation von Datensätzen regelt etc.

- 5 Die mit Peer bezeichneten Elemente Peer A, Peer B, ..., Peer N des P2P Netzwerkes sind beispielsweise selbständige Rechner, die untereinander beispielsweise sowohl über IP-Protokoll als auch über P2P Protokoll miteinander verbunden sind. Die hier vorausgesetzte Technologie eines P2P Netzwerkes ist bei-
- 10 spielsweise aus einer Diplomarbeit von Thomas Frieze an der Philipps-Universität Marburg zum Thema - Selbstorganisierten- de Peer-to-Peer Netzwerke vom März 2002 bekannt. Innerhalb des IP-Netzes kann ebenso ein Server bzw. Zertifikatsserver beispielsweise eines Diensteanbieters angeordnet
- 15 sein.

- Der Gegenstand der Erfindungen wird anhand der nachfolgenden Figurenbeschreibung verdeutlicht. Ein mit Peer X bezeichnetes Netzelement soll dabei beispielsweise Zugang zu Netzteilneh-
- 20 mern eines mit P2P bezeichneten Netzwerkes erhalten.

- In Figur 2 wird schematisch der Zugang des Netzteilnehmers Peer X zum P2P Netzwerk erläutert. In einem ersten Verfahrensschritt wird vom Netzteilnehmer Peer X, der beispielsweise ein Rechner sein kann, ein Zertifikat ZX von einem Anbieter FIRM angefordert bzw. beantragt. Der Anbieter FIRM sendet dem Antragsteller Peer X das zugeteilte und ebenfalls im Zertifikatsserver CA hinterlegte Zertifikat. Dieses vom Zertifikatsserver angelegte Zertifikat ZX für den Netzteilnehmer Peer
- 25 X besteht beispielsweise aus verschiedenen Rubriken wie Name des Anbieters, der Firma oder des Trustcenters der das Zertifikat vergibt, einer Seriennummer des Zertifikates, einen öffentlichen Schlüssel von Peer X, einem Gültigkeitszeitraum, einem Namen, wem der Schlüssel (Peer X) gehört und eine Sig-
- 30 natur, die von dem Anbieter oder Trustcenter erzeugt wird. Mit der Signatur wird sichergestellt, dass die in dem Zertifikat hinterlegten Daten nur von dem Trustcenter bzw. der

Firma oder dem Anbieter vergeben wurden. Dieses Zertifikat ZX wird in einem zweiten Schritt an den neuen Netzteilnehmer Peer X des P2P-Netzwerkes gesendet. Ebenso wird vom Zertifikatsserver CA, der das P2P-Netzwerk als Ganzes betrachtet, das Zertifikat ZX auch an das P2P-Netzwerk gesendet. Beispielsweise sendet der Zertifikatsserver CA das Zertifikat ZX dazu an den Peer A. Das Peer A kann hierbei eine Gatewayfunktion übernehmen. Das Zertifikat ZX wird dann innerhalb des P2P Netzwerkes als Ressource beispielsweise im Peer M abgespeichert.

Mit der Abspeicherung des digitalen Zertifikats als Ressource im P2P-Netzwerk stehen die Informationen des digitalen Zertifikates auch dann den Netzteilnehmern des P2P Netzwerkes zur Verfügung, wenn die Netzeinheit Peer X im Betriebsmodus Offline oder aus anderen Gründen nicht erreichbar ist. Die Gültigkeitsdauer dieser Ressource entspricht dabei der Gültigkeitsdauer des Zertifikates. Somit ist es möglich, auf einen öffentlichen Schlüssel, der im Zertifikat hinterlegt ist, zuzugreifen, um die in einer Netzeinheit im P2P Netzwerk hinterlegte und signierte Informationen auf deren Authentizität hin zu überprüfen. Die Autorisierung des Zertifikatsverwenders ergibt sich aus dem Besitz eines gültigen Zertifikates, welches vom Anbieter FIRM ausgegeben wurde. Des weiteren ist es auch möglich, für einen Netzteilnehmer bestimmte Information verschlüsselt und somit geschützt im P2P-Netz abzulegen. Damit könnte beispielsweise eine vertrauliche Anruferbeantworterfunktion realisiert werden.

In Figur 3 ist schematisch wiedergegeben, wie der Netzteilnehmer Peer C eine Nachricht von Netzteilnehmer Peer X erhält, deren Authentizität von Peer C geprüft werden soll. Dazu benötigt Peer C das Zertifikat ZX von Peer X. Dieses Zertifikat ZX extrahiert Peer C aus dem P2P Netzwerk und lädt es in seinen Speicher: Dazu bestimmt Peer C die Identifikation ID des Zertifikats ZX, nach der im verwendeten P2P Algorithmus festgelegten Methode, und sucht anschließend mit der im

verwendeten P2P Algorithmus festgelegten Methode nach einem Peer, dessen Identifikation mit der ID des Zertifikates möglichst gut übereinstimmt, und in dessen Speicher das Zertifikat ZX daher abgelegt wurde.

5 Nachdem das Zertifikat ZX in der Ressource des Netzteilnehmers Peer M gefunden wurde, wird das Zertifikat ZX an den suchenden Netzteilnehmer Peer C gesendet. Dieser überprüft nun zuerst die Gültigkeit des Zertifikates ZX mittels des öffentlichen Schlüssels QCA aus dem Rootzertifikat ZCA; anschließend prüft er die Authentizität der Nachricht mittels des öffentlichen Schlüssels QX, welcher im Zertifikat ZX enthalten ist. Ist die Authentizität bestätigt, wird die Nachricht bearbeitet; ansonsten wird sie ignoriert.

15 In Figur 4 ist schematisch der Aufbau eines Netzteilnehmers Peer A beschrieben. Für das Verständnis der Erfindung sind in die Darstellung ein Netzwerkmodul NWM, ein erstes Speichermodul SMPA, SMCA, SMA,.. und ein zweites Speichermodul SMX, SMY,..., ein Kryptomodul KRM sowie ein mit diesen Modulen in
20 Verbindung stehender Prozessor P aufgenommen. Das Netzwerkmodul NWM mit Netzwerkkarte und dazugehöriger Software etc. regelt die Kommunikation mit allen externen Geräten, z.B. zwischen Peers im P2P-Netzwerk sowie auf der Internetprotokollbasierten IP-Ebene. In dem Speichermodul SMPA ist ein privater Schlüssel PA von Peer A abgespeichert; dieser muss vom
25 Peer A geheim gehalten werden. Im Speichermodul SMA ist das Zertifikat von Peer A mit öffentlichem Schlüssel QA sowie im Speichermodul SMCA ist ein Zertifikat von Server CA mit öffentlichem Schlüssel QCA. Diese ersten 3 Datensätze sind in
30 jedem Peer immer vorhanden. In einem zweites Speichermodul sind Zertifikate von anderen Peers X,Y,... abgelegt; diese werden bei Bedarf aus dem P2P-Netzwerk geholt. Das Kryptomodul KRW, das Software- und/oder Hardwaremäßig ausgebildet ist, verfügt dabei über Funktionen wie: Erzeugung einer digitalen Signatur mit Hilfe des privaten Schlüssels PA. Authentizitätsprüfung der digitalen Signatur von beliebigem Peer X
35 mittels dessen öffentlichen Schlüssel QX, welcher im Zertifi-

kat von X enthalten ist. Gültigkeitsprüfung eines digitalen Zertifikates über die Authentizitätsprüfung seiner digitalen Signatur, erstellt vom Server CA mittels dessen öffentlichen Schlüssel QCA, welcher im (Root-) Zertifikat von CA enthalten ist. Verschlüsselung einer vertraulichen Nachricht an Peer X mittels des öffentlichen Schlüssels QX aus dem Zertifikat von Peer X. Entschlüsselung einer vertraulichen Nachricht von Peer X an Peer A mittels des privaten Schlüssels PA von Peer A.

In Figur 5 ist ein Programmablauf einer Zertifikatsverteilung wie in Fig.2 schematisch dargestellt wiedergegeben. Zur Zertifikatsverteilung sei in einer Vorbemerkung angegeben, dass alle Netzteilnehmer im P2P-Netzwerk ein selbstsigniertes Zertifikat des Zertifikatserzeugungsservers CA fest integriert haben. Damit hat jeder Netzteilnehmer einen öffentlichen Schlüssel QCA des Zertifikatserzeugungsservers CA. Alle Peers A, B,...N haben weiterhin eine Identifikation ID, diese Identifikation ID ist beispielsweise die Netzwerk-Adresse in dem genannten P2P-Netzwerk. Der Zertifikatserzeugungsserver CA hat das Zertifikat ZX für den Netzteilnehmer Peer X des P2P Netzwerkes erzeugt, d.h. mit seinem privaten Schlüssel PCA des Servers signiert. Dieses Zertifikat bindet einen öffentlichen Schlüssel QX an dessen Identität X.

Eine Zertifikatsverteilung erfolgt danach nach folgenden Verfahrensschritten: Der Server sendet ein Zertifikat an einen bestimmten Peer. Im vorliegenden Beispiel ist dieser der Peer A im P2P Netzwerk. Im Peer A kann die Signatur des Zertifikats ZX mittels des ihm bekannten öffentlichen Schlüssels QCA geprüft werden. Falls die Signatur als ungültig festgestellt wird, wird das Zertifikat nicht weitergeleitet, sondern gelöscht. Auch ist es möglich, dass der Zertifikats-Server selbst ein solcher Netzteilnehmer im P2P-Netzwerk ist.

In Peer A wird die Identifikation ID, die bestimmt auf welchen Peers eine Ressource im P2P Netzwerk abgelegt wird, des

Zertifikates ZX nach einer in P2P Netzwerken üblichen Methode festgelegt, die vom verwendeten P2P Algorithmus/Protokoll abhängt. Zu P2P Algorithmen/Protokollen siehe beispielsweise Petar Maymounkov, David Mazieres, New York University, Kademlia: A Peer to Peer Information System Based on XOR Metric, 2001

oder Stoica, Morris, Karger, Kaashoek, Balakrishnan, MIT Laboratory for Computer Science: Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications, August 2001.

Beispielsweise berechnet der Peer A diese ID des Zertifikates derart, dass sie aus einer eindeutigen Kennzeichnung vom Peer X hervorgeht, so dass das Zertifikat allein unter Kenntnis dieser Kennzeichnung im P2P Netz gefunden und extrahiert werden kann.

Peer A sucht sich innerhalb des P2P-Netzwerkes den Peer M, dessen Identifikation ID mit der ID des Zertifikates am besten übereinstimmt. Die Übereinstimmung bezieht sich auf eine Metrik des P2P-Netzwerksystems.

Der Peer A sendet das Zertifikat ZX an Peer M.

Im Rechner Peer M kann die Signatur des Zertifikates mittels des öffentlichen Schlüssels QCA auch überprüft werden. Ist diese o.k., speichert er das Zertifikat ab, ansonsten wird das Zertifikat gelöscht.

Das Zertifikat von Peer X ist im P2P-Netzwerk wie oben beschrieben als Ressource verfügbar, d.h. es kann von jedem Peer A,B,...N, der es benötigt, im P2P-Netzwerk gesucht und extrahiert werden. Die Erfindung bringt somit den Vorteil mit sich, dass das Zertifikat ZX auch dann noch verfügbar ist, wenn der Server und Peer X nicht verfügbar sind.

In Figur 6 ist schematisch ein Ablaufdiagramm einer Authentizitätsprüfung wiedergegeben. Zur Authentizitätsprüfung sei

angemerkt, dass alle Peers im P2P-Netzwerk selbstsignierte Zertifikate des Zertifikatserzeugungsservers CA fest integriert haben. Damit hat jeder Peer A,B,... N, einen öffentlichen Schlüssel QCA des Zertifikatserzeugungsservers CA. Alle
5 Peers A,B,...,N, haben eine Identifikation ID, die als Netzwerkadresse im P2P-Netzwerk dient. Das Zertifikat für Peer X liegt als Ressource im P2P-Netz. So kann beispielsweise ein Datensatz wie beispielsweise ein Datenfile, Serviceanfrage oder Nachricht..., von dem Peer X mit seinem privaten Schlüssel PX signiert und an Peer C gesendet oder im P2P-Netzwerk
10 in einem anderen Rechner Peer M, ..., Peer N, abgelegt werden. Der Peer C erhält diesen Datensatz vom Peer X oder von einem dritten Rechner Peer M.

15 Peer C benötigt jetzt zur Authentizitätsprüfung, also zur Prüfung, dass der Datensatz also wirklich von Peer X stammt, dessen Zertifikat ZX.

Peer C bestimmt z.B. aus einer eindeutigen Kennzeichnung von
20 Peer X die Identifikation ID des Zertifikates von Peer X.

In einem nachfolgenden Verfahrenabschnitt sucht Peer C mit dieser ID einen Netzteilnehmer, auf dem das Zertifikat gespeichert ist, und erhält Peer M als Ziel.

25 Der Rechner Peer C veranlasst Peer M, ihm das Zertifikat zu schicken. In Peer C wird nun die Gültigkeit des Zertifikates ZX überprüft und anschließend die Authentizität des von Peer X erhaltenen Datensatzes geprüft. Falls das Zertifikat und
30 die Authentizität o.k. sind, bearbeitet Peer C den Datensatz, der von Peer X gesendet wurde. Damit ist auch eine Zugangskontrolle des P2P Netzes möglich: Nur Teilnehmer, die ein Zertifikat, vom Zertifikatserzeugungsserver CA erhalten haben, sind autorisiert, Datensätze zur Bearbeitung durch andere Teilnehmer zu erzeugen.
35

Aufgrund der Hinterlegung des Zertifikates in den Ressourcen

des P2P-Netzes kann jeder Peer A,B,..N, nun die Authentizität von Datensätzen im Netz im P2P-Netzwerk überprüfen. Die Überprüfung kann auch dann noch abgewickelt werden, wenn der Server und der Netzteilnehmer Peer X nicht verfügbar sind.

5

In Figur 7 ist schematisch der Ablauf einer verschlüsselten Hinterlegung wiedergegeben. Der nachfolgende Ablauf einer verschlüsselten Hinterlegung erfolgt ähnlich der wie zuvor beschriebenen Authentizitätsprüfung. Ausgehend von Peer C soll eine verschlüsselte Nachricht an Peer X im Netzwerk hinterlegt werden. Der Rechner Peer C bestimmt z.B. aus einer eindeutigen Kennzeichnung von Peer X die ID des Zertifikates von Peer X. Der Rechner Peer C sucht mit dieser ID einen Peer auf dem das Zertifikat gespeichert ist, und erhält Peer M als Ziel. Der Rechner Peer C veranlasst Peer M, ihm das Zertifikat zu schicken. Peer C überprüft die Gültigkeit des Zertifikates von Peer X. In Peer C wird die Nachricht mit dem öffentlichen Schlüssel QX aus dem Zertifikat von Peer X verschlüsselt. Der Peer C kann nun die verschlüsselte Nachricht im P2P-Netz hinterlegen.

20

Wenn Peer X die verschlüsselte Nachricht erhält, kann nur Peer X mit seinem privaten Schlüssel PX die an ihn gerichtete Nachricht von Peer C entschlüsseln.

25

Mit diesem Ablauf einer verschlüsselten Hinterlegung kann jeder Peer A,B,..Peer N, verschlüsselte Nachrichten an andere Teilnehmer des P2P-Netzwerkes senden bzw. hinterlegen. Dieses Senden bzw. Hinterlegen von Nachrichten an andere Teilnehmer des P2P-Netzwerkes kann unabhängig von einem Server oder der Erreichbarkeit des Ziel-Peers erfolgen.

30

Verfahren zur sicheren Kommunikation von Geräten bzw. Netzteilnehmern in P2P-Netzen. In diesen Netzen werden Zertifikationsinformationen über Geräte und Anwender benötigt, um von diesen signierte Informationen auf deren Authentizität hin zu überprüfen, sowie um vertrauliche Informationen an sie ver-

35

schlüsselt zu übertragen. Wer diese Zertifikationsinformationen benötigt, kann sie vom Netzteilnehmer selbst oder von externen Servern anfordern. Gemäß der Erfindung wird diese Information zusätzlich als Ressource im P2P-Netzwerk abgelegt.

5 Dies bringt den Vorteil mit sich, dass die Informationen auch dann verfügbar sind, wenn das Gerät- der Anwender nicht erreichbar sind und kein Server zur Verfügung steht. Dies bringt ebenso den weiteren Vorteil mit sich, dass die Authentizitätsprüfung dauerhaft gewährleistet ist und außerdem In-

10 formationen auch dann vertraulich hinterlegt werden, wenn Gerät und Anwender temporär nicht erreichbar sind.

Patentansprüche

1. Schaltungsanordnung zur Kommunikationssicherheit zwischen zu einem Peer-to-Peer Netzwerk gehörenden Netzteilnehmern,
5 mit
einem Netzwerkmodul zur Kommunikation mit den weiteren Netzteilnehmern und externen nicht zum Peer-to-Peer Netzwerk gehörenden Kommunikationseinrichtungen (Server),
einem Kryptomodul zur Abwicklung von kryptographischen Aufgaben,
10 einem ersten Teilspeichermodul aufweisenden Speichermodul (SM1) in denen zu einem ersten Netzteilnehmer Zugehörigkeitsmerkmale (PA, ZA, ZCA) abgespeichert sind, dadurch gekennzeichnet,
dass ein zweites Speichermodul (SM2) vorgesehen ist, wobei
15 das zweite Speichermodul (SM2) Teilspeichermodule (SMX, SMY,...) zur Zwischenspeicherung von Zertifikaten (ZX, ZY,...) weiterer Netzteilnehmer (Peer X, Peer Y,.....) aufweist und die Zertifikate dieser weiteren Netzteilnehmer jeweils von allen anderen Netzteilnehmern (Peer N, Peer M,.....) angefordert werden können.
20

2. Schaltungsanordnung nach Anspruch 1
dadurch gekennzeichnet,
dass die externe Kommunikationseinrichtung derart ausgeprägt
25 ist, dass digitale Zertifikate hergestellt und im zweiten Speichermodul (SM2) abgelegt werden können.

3. Schaltungsanordnung nach einem der vorhergehenden Ansprüche,
30 dadurch gekennzeichnet,
dass diese im ersten Netzteilnehmer angeordnet ist.

4. Verfahren zur Kommunikationssicherheit zwischen zu einem
35 Peer-to-Peer Netzwerk gehörenden Netzteilnehmern, mit
einem Netzwerkmodul zur Kommunikation mit den weiteren Netzteilnehmern und externen nicht zum Peer-to-Peer Netzwerk ge-

- hörenden Kommunikationseinrichtungen (Server),
einem Kryptomodul zur Abwicklung von kryptographischen Aufgaben, einem ersten Teilspeichermodul aufweisenden Speichermodul (SM1) in denen zu einem ersten Netzteilnehmer Zugehörigkeitsmerkmale abgespeichert werden,
5 dadurch gekennzeichnet,
dass ein zweites Speichermodul (SM2) in Teilspeichermodulen (SMX, SMY,...) zur Zwischenspeicherung von Zertifikaten (ZX, ZY,...) weiterer Netzteilnehmer (Peer X, Peer Y,.....) aufgeteilt wird und die Zertifikate dieser weiteren Netzteilnehmer von allen anderen Netzteilnehmern (Peer N, Peer M,....) angefordert werden können.
- 10
5. Verfahren nach Anspruch 4,
15 dadurch gekennzeichnet,
dass digitale Zertifikate in der externen Kommunikationseinrichtung erstellt werden und im zweiten Speichermodul (SM2) abgelegt werden können.

FIG 1

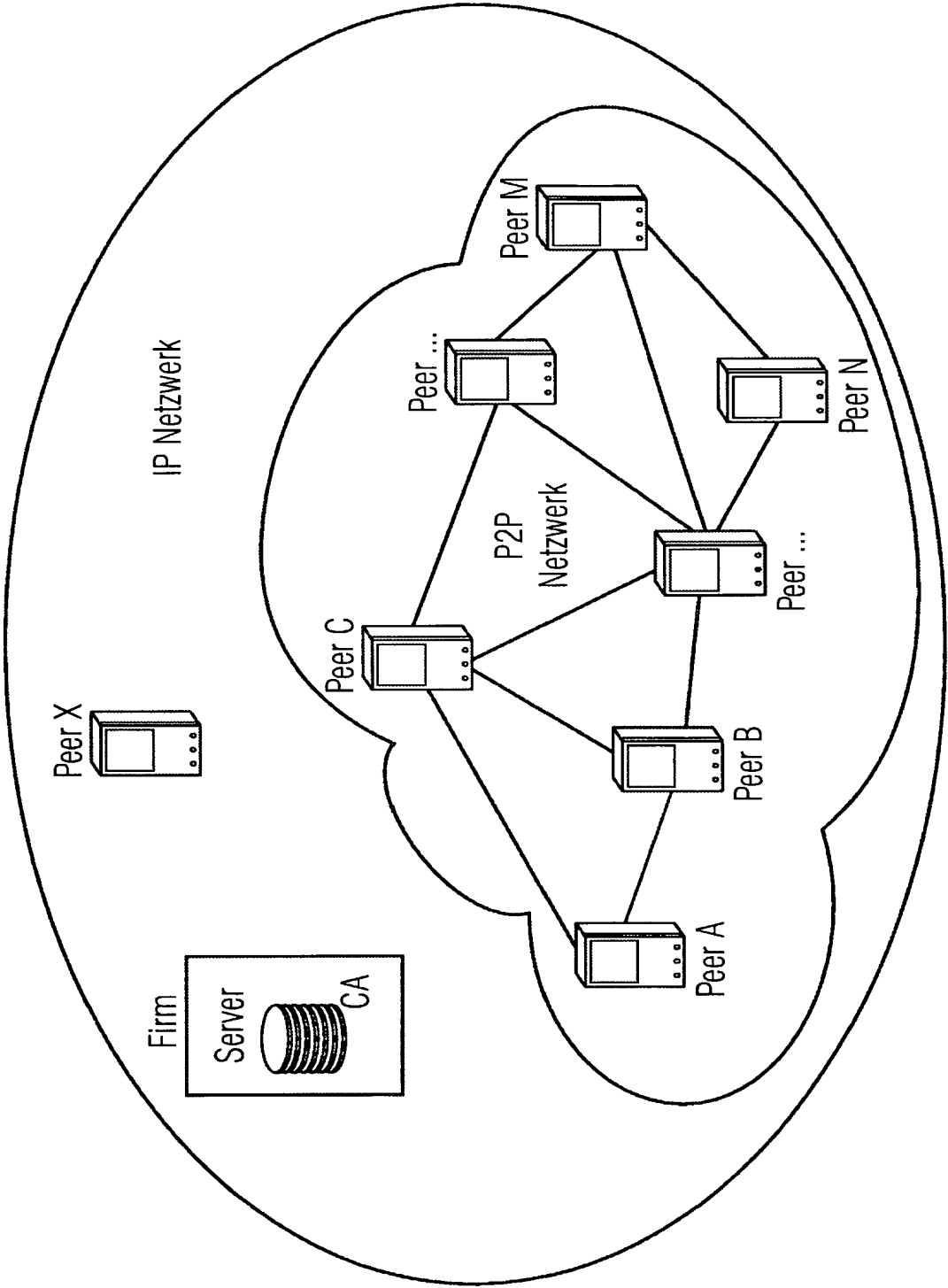


FIG 2

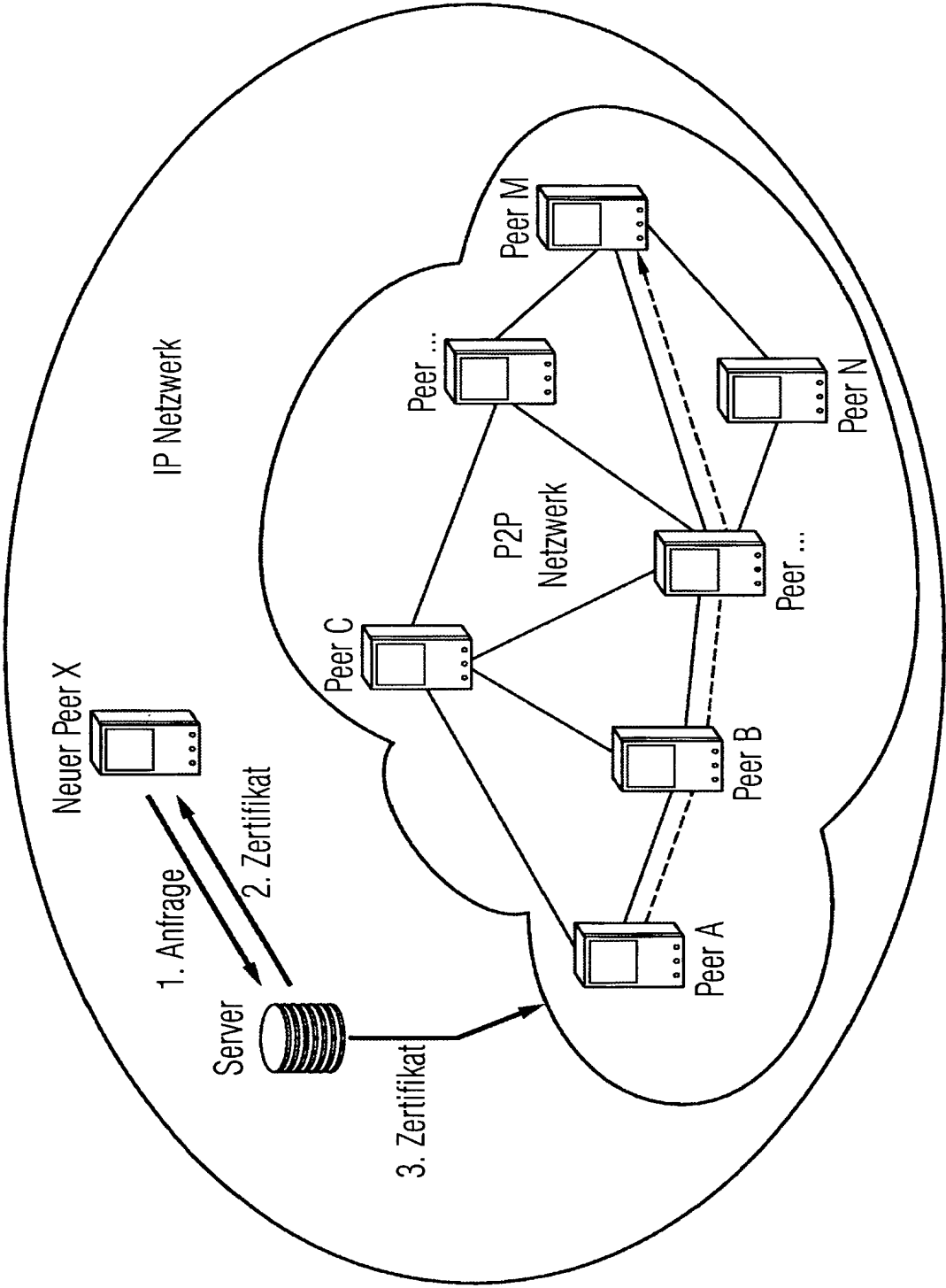


FIG 3

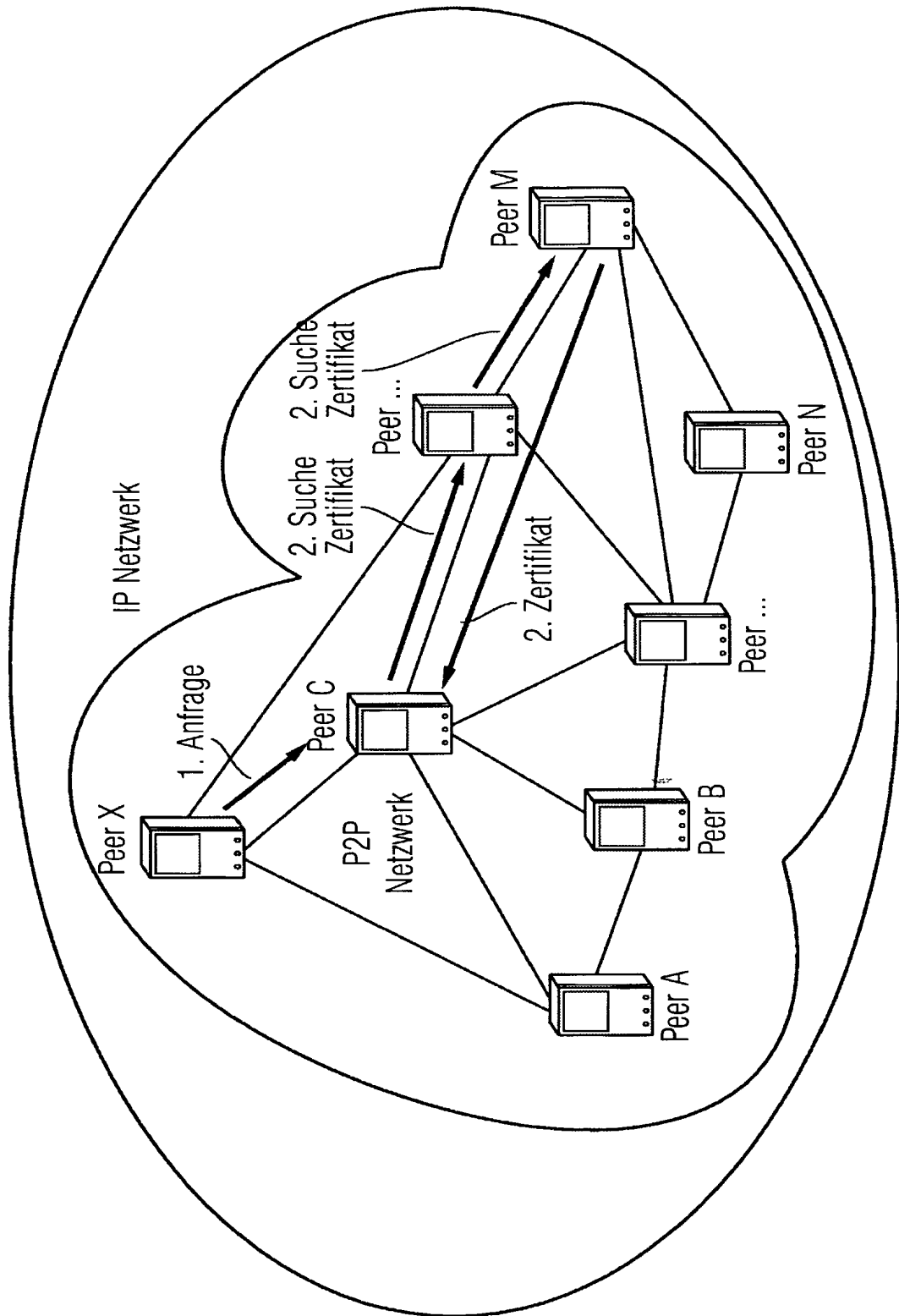
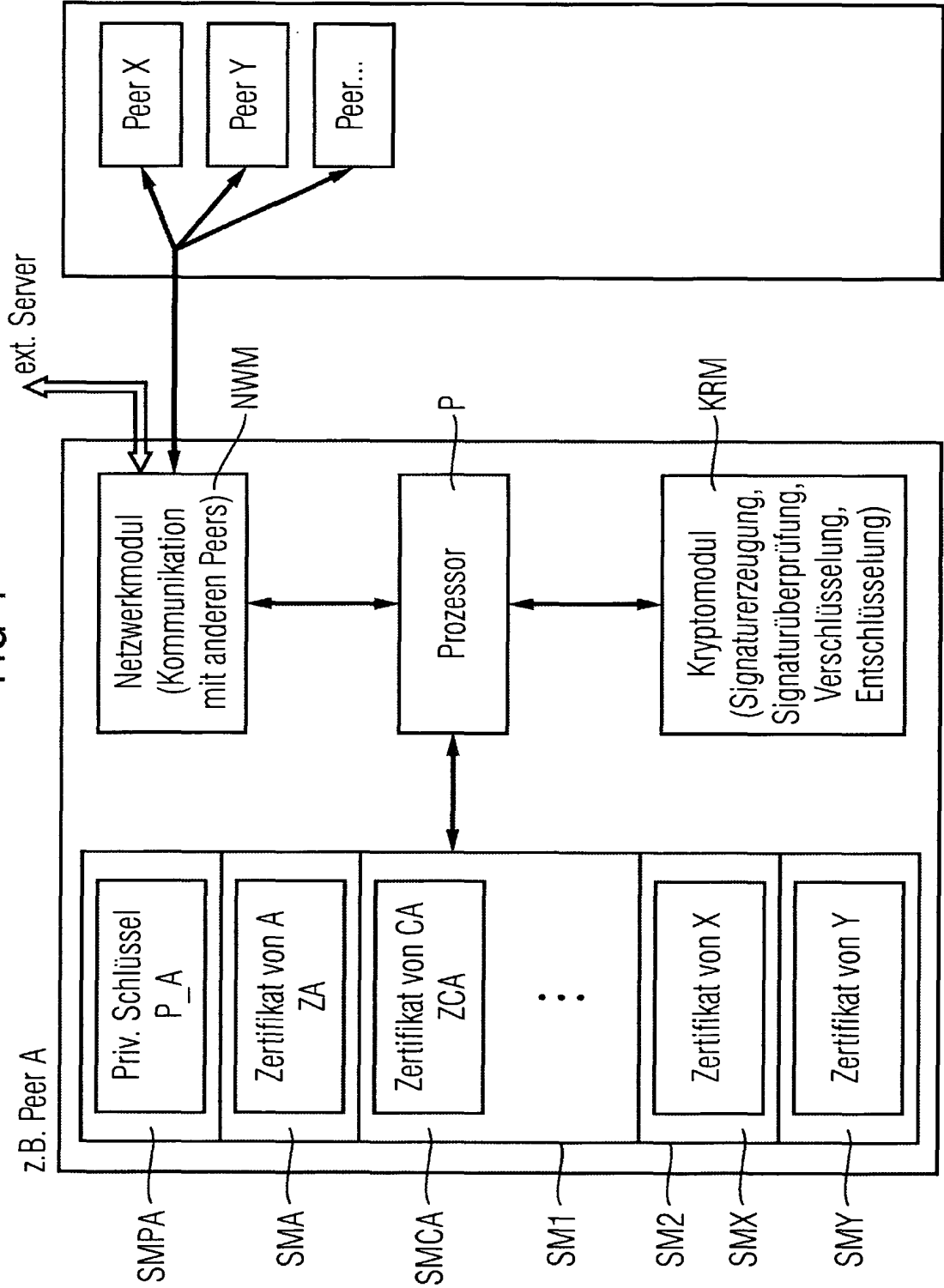


FIG 4



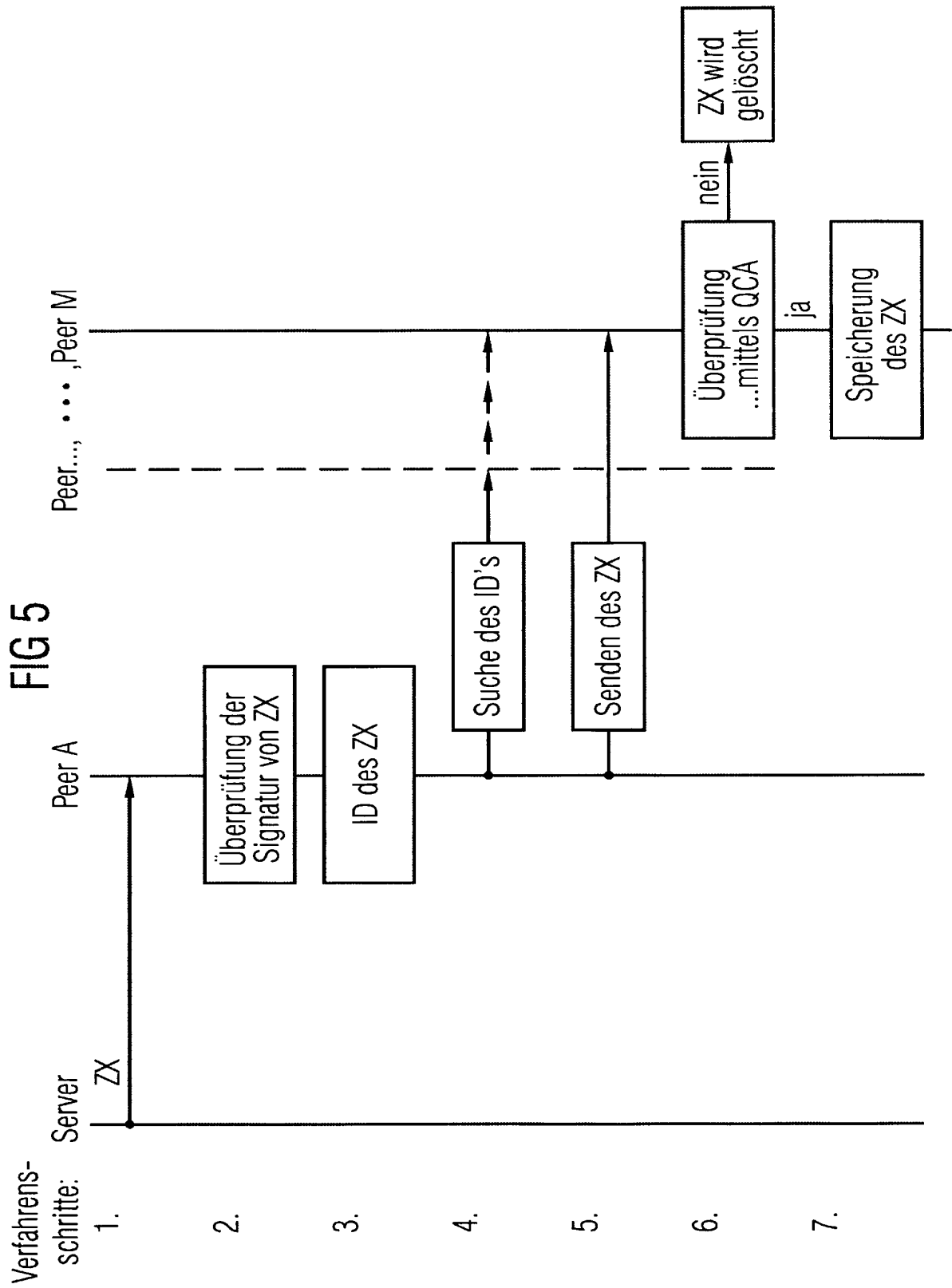
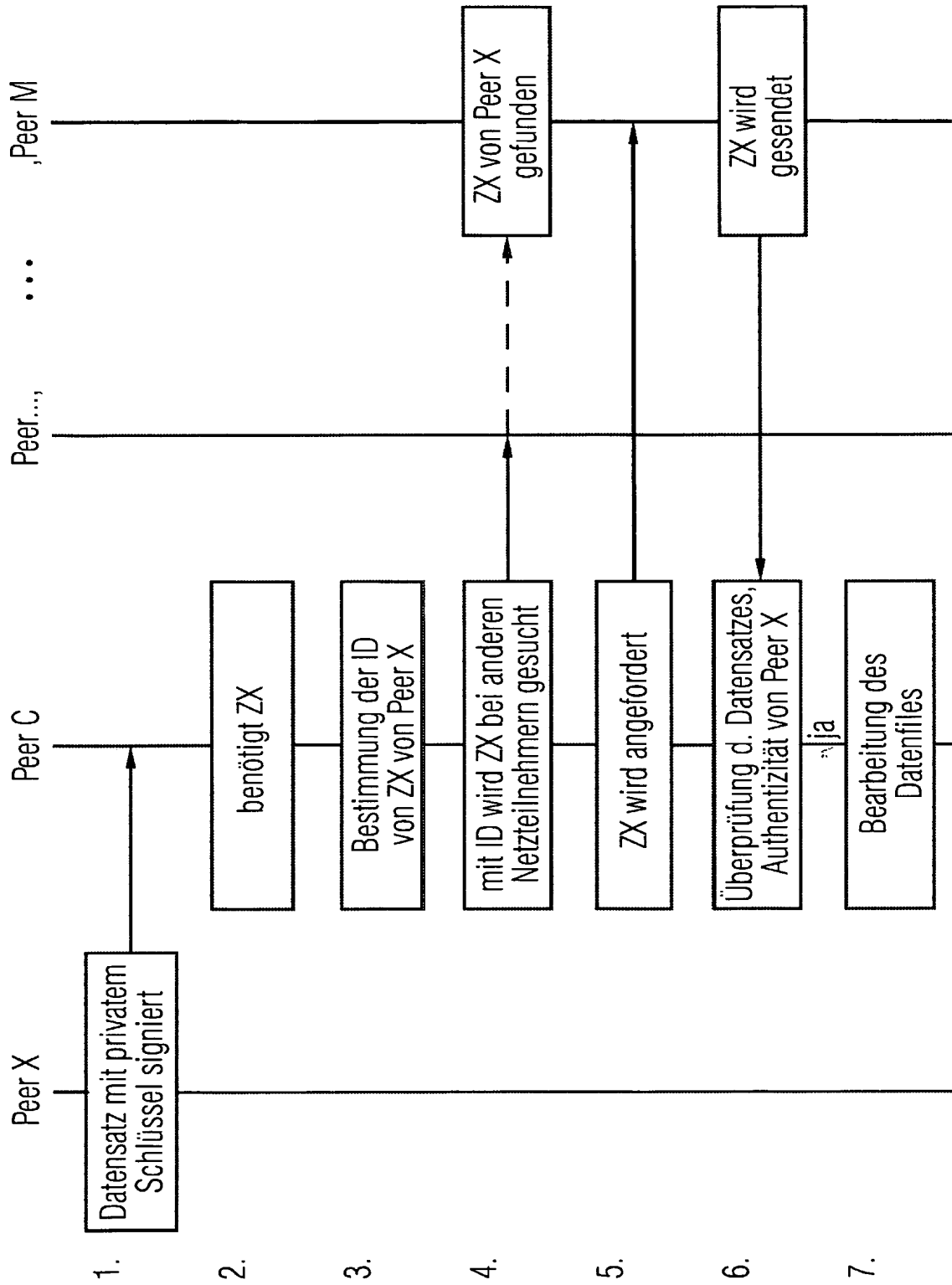
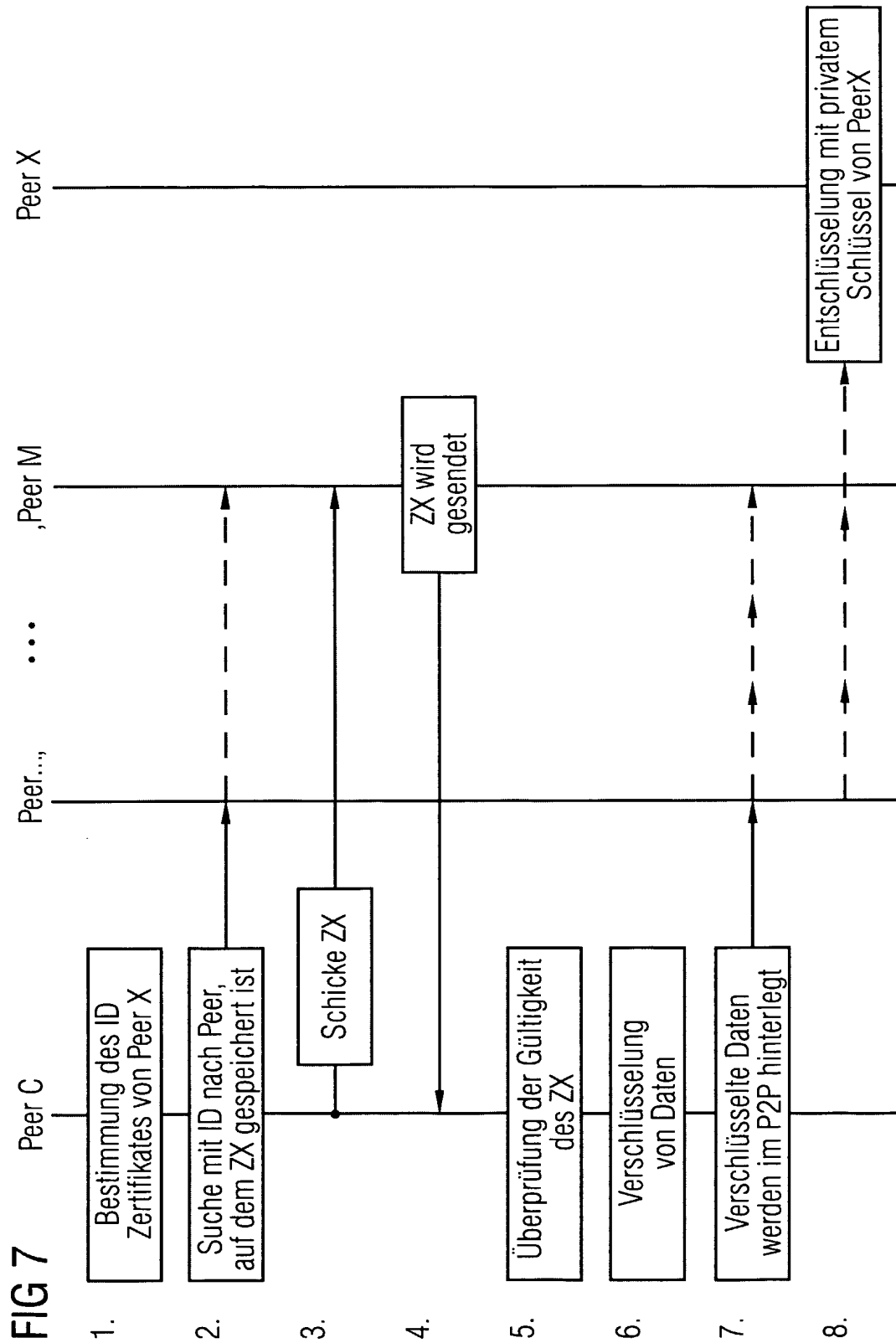


FIG 6



7/7



INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/050360

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/070070 A1 (YEAGER WILLIAM J ET AL) 10 April 2003 (2003-04-10) abstract paragraph '0054! - paragraph '0072! paragraph '0106! - paragraph '0127! paragraph '0231! - paragraph '0262! -----	1-5
A	US 2003/056093 A1 (HUITEMA CHRISTIAN ET AL) 20 March 2003 (2003-03-20) abstract paragraph '0038! - paragraph '0047! paragraph '0053! - paragraph '0061! ----- -/--	1-5

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

10 May 2005

Date of mailing of the international search report

24/05/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Apostolescu, R

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/050360

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>WOORYOUNG K ET AL: "A secure platform for peer-to-peer computing in the Internet" 7 January 2002 (2002-01-07), PROCEEDINGS OF THE HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, PAGE(S) 3948-3957 , XP002251810 the whole document</p>	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2005/050360

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003070070	A1	10-04-2003	
		EP 1229442 A2	07-08-2002
		EP 1229443 A2	07-08-2002
		EP 1282289 A2	05-02-2003
		WO 02057917 A2	25-07-2002
		US 2002143944 A1	03-10-2002
		US 2002143855 A1	03-10-2002
		US 2002184310 A1	05-12-2002
		US 2002184357 A1	05-12-2002
		US 2002184311 A1	05-12-2002
		US 2003002521 A1	02-01-2003
		US 2002152299 A1	17-10-2002
		US 2002184358 A1	05-12-2002
		US 2002188657 A1	12-12-2002
		US 2002147810 A1	10-10-2002
		US 2002147771 A1	10-10-2002
		US 2002156893 A1	24-10-2002
		US 2003028585 A1	06-02-2003
		US 2003055894 A1	20-03-2003
		US 2003055898 A1	20-03-2003
		US 2003041141 A1	27-02-2003
<hr/>			
US 2003056093	A1	20-03-2003	NONE
<hr/>			

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/050360

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/32 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RESEARCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2003/070070 A1 (YEAGER WILLIAM J ET AL) 10. April 2003 (2003-04-10) Zusammenfassung Absatz '0054! - Absatz '0072! Absatz '0106! - Absatz '0127! Absatz '0231! - Absatz '0262! -----	1-5
A	US 2003/056093 A1 (HUITEMA CHRISTIAN ET AL) 20. März 2003 (2003-03-20) Zusammenfassung Absatz '0038! - Absatz '0047! Absatz '0053! - Absatz '0061! ----- -/-	1-5

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

- *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
- *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
- *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
- *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
- *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

10. Mai 2005

Absenddatum des internationalen Recherchenberichts

24/05/2005

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Apostolescu, R

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/050360

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie ^a	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	<p>WOORYOUNG K ET AL: "A secure platform for peer-to-peer computing in the Internet" 7. Januar 2002 (2002-01-07), PROCEEDINGS OF THE HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, PAGE(S) 3948-3957 , XP002251810 das ganze Dokument -----</p>	1-5

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2005/050360

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2003070070 A1	10-04-2003	EP 1229442 A2	07-08-2002
		EP 1229443 A2	07-08-2002
		EP 1282289 A2	05-02-2003
		WO 02057917 A2	25-07-2002
		US 2002143944 A1	03-10-2002
		US 2002143855 A1	03-10-2002
		US 2002184310 A1	05-12-2002
		US 2002184357 A1	05-12-2002
		US 2002184311 A1	05-12-2002
		US 2003002521 A1	02-01-2003
		US 2002152299 A1	17-10-2002
		US 2002184358 A1	05-12-2002
		US 2002188657 A1	12-12-2002
		US 2002147810 A1	10-10-2002
		US 2002147771 A1	10-10-2002
		US 2002156893 A1	24-10-2002
		US 2003028585 A1	06-02-2003
		US 2003055894 A1	20-03-2003
		US 2003055898 A1	20-03-2003
		US 2003041141 A1	27-02-2003
<hr/>			
US 2003056093 A1	20-03-2003	KEINE	
<hr/>			